UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/859,608	05/17/2001	Pankaj B. Patel		4992

27300 7590 10/19/2006

PANDISCIO & PANDISCIO, P.C.
470 TOTTEN POND ROAD
WALTHAM, MA 02451-1914

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/859,608	PATEL, PANKAJ B.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *7/31/2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6-8 and 10* is/are pending in the application.

4a) Of the above claim(s) *2-5,9 and 11* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,6-8 and 10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 2-5, 9, and 11 have been cancelled. Applicant's arguments/amendments with respect to previously presented claims 1, 6-8, and 10 filed 7/31/2006 have been fully considered but are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Applicants contend that Park et al. do not disclose "comparing, at the central server, the first and second cryptogram." Examiner respectfully disagrees. Park teaches that the central server sends a random number to the client who operated on that number and sends it back to the server (par. 31). Park et al. then teach that the central server must operate on the values sent back from the client by decrypting the data that is sent to the server (par. 32). Finally, Park et al. teach that from the decrypted values, the server extracts one of the values (the random number sent to the client and included in what could be the first cryptogram) and compares it with the original value of the random number calculated by the server (par. 33). Once these cryptograms are compared, the server will know whether or not the client is a malicious attacker. Therefore, Park et al., as used to modify Bianco et al., suggests motivation for comparing, at the central server, the first and second cryptograms. Park et al. suggest that keeping track of these elements can achieve robustness against attacks (par. 38).

Due to the reasons stated above, the Examiner maintains rejections with respect to all pending claims. Bianco et al. teach the limitations that the Applicant suggests distinguish from the prior art. Furthermore, Park et al. in combination with Bianco et al. teach the limitations not

explicitly disclosed by Bianco et al. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 6, 8, and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bianco et al., US Patent No. 6,256,737, and further in view of Park et al., US Pub. No. 2002/0073322.

As per claims 1 and 11:

Bianco substantially teaches a method/system for authenticating a user over a network, comprising the steps of providing an identification box at the local site of the user, and providing a central server at a remote site, with the identification box including a biometric reader, and with the identification box and the central server being connected over the network (col. 12, lines 12-22); confirming the identity of the user to the central server, using the identification box (fig. 8A, elements 802 and 804); measuring a first biometric parameter from the user with the biometric reader, and storing the first biometric parameter in encrypted form at the identification box (col. 8, lines 1-40) and at the central server (col. 10, lines 1-27); sending a user request for authentication from the identification box to the central server (fig. 8A, elements 802, 804, and 806); measuring a second biometric parameter from the user with the biometric reader;

encrypting the second biometric parameter (col. 8, lines 16-17); comparing, at the identification box, the second encrypted biometric parameter with the previously-stored first encrypted biometric parameter (col. 26, lines 8-33).

Not explicitly disclosed is sending a unique math table and a random number from the central server to the identification box, with the unique math table being stored at both the central server and the identification box; operating on the random number, at the identification box, with the unique math table to create a first cryptogram when a positive match occurs between the first and second encrypted biometric parameters; and sending the first cryptogram from the identification box to the central server. However, Park et al. teach that the central server sends a random number and table to the client computer who uses that information to create another random number that is then encrypted and sent back to the server. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method/system disclosed in Bianco et al. for the server to send the unique table and random number to the client's identification box at the client terminal and use that information for creating a first cryptogram. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Park et al. suggest that these techniques can be used in a system in order for the server to achieve robustness against an attack in paragraphs 38-39 and 42-50.

Finally not explicitly disclosed is operating on the random number, at the central server, with the unique math table to create a second cryptogram and comparing, at the central server, the first cryptogram with the second cryptogram; and confirming the authenticity of the user when a positive match occurs between the first cryptogram and the second cryptogram.

However, Park et al. teach that the server uses the stored table and the random number to recalculate a second cryptogram and compares that with the first cryptogram, thereby confirming the authenticity of the user when a positive match occurs between the two cryptograms. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method/system disclosed in Bianco et al. for the server to calculate a second cryptogram and compare that to the first cryptogram transmitted by the client terminal allowing the server to authenticate the user when a positive match results. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Park et al. suggest that these techniques can be added to a system in order for the server to achieve robustness against an attack in paragraphs 38-39 and 51-53.

As per claim 6:

Bianco et al. and Park et al. substantially teach the method as in claim 1. Furthermore, Park et al. teach the method further comprising the step of allowing the user access to a second remote site if the first cryptogram matches the second cryptogram (par. 53).

As per claim 7:

Bianco substantially teaches a method for authenticating a user over a network, comprising the steps of providing an identification box at the local site of the user, and providing a central server at a remote site, with the identification box including a biometric reader, and with the identification box and the central server being connected over the network (col. 12, lines 12-22); confirming the identity of the user to the central server, using the identification box (fig. 8A, elements 802 and 804); measuring a first biometric parameter from the user with the

biometric reader, and storing the first biometric parameter in encrypted form at the identification box (col. 8, lines 1-40) and at the central server (col. 10, lines 1-27); sending a user request for authentication from the identification box to the central server (fig. 8A, elements 802, 804, and 806); measuring a second biometric parameter from the user with the biometric reader; encrypting the second biometric parameter (col. 8, lines 16-17); comparing, at the identification box, the second encrypted biometric parameter with the previously-stored first encrypted biometric parameter (col. 26, lines 8-33).

Not explicitly disclosed is sending a unique math table and a random number from the central server to the identification box, with the unique math table being stored at both the central server and the identification box; generating, at the identification box a second random number when the first encrypted biometric parameter does not positively match the second encrypted biometric parameter; operating on the random number, at the identification box, with the unique math table to create a first cryptogram when a positive match fails to occur between the first and second encrypted biometric parameters; and sending the first cryptogram from the identification box to the central server. However, Park et al. teach that the central server sends a random number and table to the client computer who uses that information to create a second random number that is then encrypted and sent back to the server. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bianco et al. for the server to send the unique table and random number to the client's identification box at the client terminal and use that information for creating a first cryptogram. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Park et al. suggest

that these techniques can be used in a system in order for the server to achieve robustness against an attack in paragraphs 38-39 and 42-50.

Finally not explicitly disclosed is operating on the random number, at the central server, with the unique math table to create a second cryptogram and comparing, at the central server, the first cryptogram with the second cryptogram; and denying the authenticity of the user when there is no match between the first cryptogram and the second cryptogram. However, Park et al. teach that the server uses the stored table and the random number to recalculate a second cryptogram and compares that with the first cryptogram, thereby confirming the authenticity of the user when a positive match occurs between the two cryptograms. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bianco et al. for the server to calculate a second cryptogram and compare that to the first cryptogram transmitted by the client terminal allowing the server to deny the authenticity of the user when a positive match results. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Park et al. suggest that these techniques can be added to a system in order for the server to achieve robustness against an attack in paragraphs 38-39, 51, and 54.

As per claim 8:

Bianco et al. and Park et al. substantially teach the method as in claim 7. Furthermore, Park et al. teach the method further comprising the step of denying the user access to a second remote site if the first cryptogram does not match the second cryptogram (par. 53).

As per claim 10:

Bianco et al. and Park et al. substantially teach the method according to claim 1. Bianco

et al. further teach providing a second identification box at a second remote site, with the second identification box including a second biometric reader, and with the second identification box and the central server being connected over the network (col. 12, lines 12-22); and sending a user request for authentication from the second identification box to the central server (fig. 8A, elements 802, 804, and 806).

Not explicitly disclosed is the method further comprising: measuring a third biometric parameter from the user with the second biometric reader; encrypting the third biometric parameter; and comparing, at the second identification box, the third encrypted biometric parameter with the first encrypted biometric parameter. However, Bianco et al. teach measuring a first biometric parameter from the user with a first biometric reader, and storing the first biometric parameter in encrypted form at the first identification box (col. 8, lines 1-40) and at the central server (col. 10, lines 1-27); measuring a second biometric parameter from the user with the biometric reader; encrypting the second biometric parameter (col. 8, lines 16-17); comparing, at the first identification box, the second encrypted biometric parameter with the previously-stored first encrypted biometric parameter (col. 26, lines 8-33). Furthermore, Bianco et al. teach that there are several identification boxes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bianco et al. to measure and compare the first biometric parameter with the third biometric parameter which is merely another biometric sample from a different identification box. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Bianco et al. suggest that there exist more than one identification box in a system, as well as more than one attempt to gain access, in col. 12,

lines 11-45.

Also not explicitly disclosed is sending the unique math table and the first encrypted biometric parameter from the central server to the second identification box; sending a second random number from the central server to the second identification box; operating on the second random number, at the second identification box, with the unique math table to create a third cryptogram when a positive match occurs between the first and the third encrypted biometric parameters. However, Park et al. teach that the central server sends a second random number and table to the second client computer who uses that information to create another random number that is then encrypted and sent back to the server. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bianco et al. for the server to send the unique table and second random number to the client's second identification box at the client terminal and use that information for creating a third cryptogram. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Park et al. suggest that these techniques can be used in a system in order for the server to achieve robustness against an attack in paragraphs 38-39 and 42-50.

Finally not explicitly disclosed is operating on the second random number, at the central server, with the unique math table to create a fourth cryptogram; sending a third cryptogram from the second identification box to the central server; comparing, at the central server, the third cryptogram with the fourth cryptogram; and confirming the authenticity of the user when a positive match occurs between the third cryptogram and the fourth cryptogram. However, Park et al. teach that the server uses the stored table and the random number to recalculate a fourth

cryptogram and compares that with the third cryptogram sent by the second identification box, thereby confirming the authenticity of the user when a positive match occurs between the two cryptograms. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Bianco et al. for the server to calculate a fourth cryptogram and compare that to the third cryptogram transmitted by the second client terminal allowing the server to confirm the authenticity of the user when a positive match occurs between the third cryptogram and the fourth cryptogram. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Park et al. suggest that these techniques can be added to a system in order for the server to achieve robustness against an attack in paragraphs 38-39, and 51-53.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US Patent No. 6,002,769 has been cited because it is relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2137
10/16/2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

NK